Department of Homeland Security Daily Open Source Infrastructure Report for 16 August 2007

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- Pfizer, the world's largest drug maker, reports that for the second time in two months, a security breach has put the personally identifying information on current and former employees at risk. (See item 6)
- U.S. Customs officials said Tuesday, August 14, they had traced the source of last weekend's system outage that left 17,000 international passengers stranded in airplanes at Los Angeles International Airport to a malfunctioning network interface card on a single desktop computer in the Tom Bradley International Terminal. (See item 12)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *August 14, Platts Energy Bulletin* — **FERC proposes to approve three new NERC reliability standards.** The U.S. Federal Energy Regulatory Commission (FERC) is proposing to approve three new reliability standards developed by the North American Electric Reliability Corp. (NERC). The electric reliability organization told FERC in a November proposal that the three standards would ensure that system operating limits and interconnection reliability operating limits are developed by transmission operators using consistent methods that contain "certain essential elements." In a notice of proposed rulemaking issued late Monday, August 13, FERC

proposed to accept the three standards, but asked for comment on how consistent the requirements would be with open access transmission tariffs. The commission also said that it is prepared to accept a list of regional differences proposed by the Western Electricity Coordinating Council (WECC), saying it appears that the changes would impose more stringent requirements than those offered by NERC. FERC, however, said it is concerned that WECC has not identified a process for making changes that ensures adequate public participation.
Source: http://www.platts.com/Electric%20Power/News/6424586.xml?sub=Electric%20Power&p=Electric%20Power/News&?undefined&undefine d

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *August 15, Houston Chronicle* — **Ruptured gas line causes evacuations in north Houston.** A crew capped a broken natural gas line in Houston, on the near north side, after a construction crew accidentally ruptured it Wednesday morning, August 15. Before repairs began, firefighters briefly evacuated several homes near the intersection of Houston Avenue and Byrne. Authorities had closed Houston Avenue between White Oak and Bayland and rerouted traffic as a precaution.
Source: http://www.chron.com/disp/story.mpl/front/5055994.html

[Return to top]

Defense Industrial Base Sector

3. *August 15, Federal Computer Week* — **Security clearance reforms sought.** The Office of the Director of National Intelligence, the Department of Defense and the Office of Management and Budget are seeking ways to meet Congress' December 2009 deadline for improving the security clearance process. In a request for information (RFI) posted on the Federal Business Opportunities Website Tuesday, August 14, the Air Force, which is acting as the procurement arm for the group, is asking vendors to submit their strategies for completing 90 percent of security clearance investigations in 40 days and adjudications in 20 days. The Air Force said the new system should be in place by December 31, 2008. The RFI's goal is to find out whether industry solutions already exist that are scalable, portable and interoperable. The chosen system must work in classified and unclassified environments, and must process and track a variety of investigation types, the RFI states.
Air Force RFI: http://www.fbo.gov/spg/USAF/AFDW/11CONS/Reference%2DNumber%2DAFDWA7KIRFI1/SynopsisR.html
Source: http://www.fcw.com/article103505−08−15−07−Web

[Return to top]

Banking and Finance Sector

4. *August 15, Department of the Treasury* — **Treasury targets financial network of Ramierz Abadia.** The U.S. Department of the Treasury's Office of Foreign Assets Control on

Wednesday, August 15, added to its list of Specially Designated Narcotics Traffickers (SDNT) 23 Colombian individuals and 23 Colombian companies tied to Juan Carlos Ramirez Abadia (a.k.a. Chupeta), a leader of Colombia's North Valle drug cartel. Companies designated today include: APVA S.A., a real estate company located in Cali, Colombia; Campo a la Diversion E.U. (a.k.a. Parque Yaku), an amusement park located in Yumbo, Valle, Colombia; Criadero Santa Gertrudis S.A., a horse breeding farm in Jamundi, Valle, Colombia; and Ensambladora Colombiana Automotriz S.A., an automotive assembly company located in Barranquilla, Colombia. SDNTs are subject to the economic sanctions imposed against Colombian drug cartels in Executive Order 12978. Wednesday's designation action freezes any assets the designees may have subject to U.S. jurisdiction, and prohibits all financial and commercial transactions by any U.S. person with the designated companies and individuals.
Source: http://www.treasury.gov/press/releases/hp535.htm

5. *August 14, SecurityFocus* — **TJX estimates breach costs at $118 million.** Retail giant TJX Companies announced on Tuesday, August 14, that it would take a $118 million charge to pay for the costs and potential liability stemming from the earlier theft of some 45.6 million credit and debit accounts. The $118 million charge includes $11 million rung up during the investigation into the attacks in the second quarter of its fiscal year 2008, the company said in a statement. The remaining $107 million will be put into a reserve created to fuel the company's legal battles and pay any potential judgments, the retail giant said. The incident, announced in January, involved multiple intrusions into the company's systems by online thieves between July 2005 and January 2007.
Source: http://www.securityfocus.com/brief/568

6. *August 14, InformationWeek* — **Pfizer reports second data breach in two months.** For the second time in two months, a security breach at pharmaceutical giant Pfizer has put the personally identifying information on current and former employees at risk. The company, which is the world's largest drug maker, alerted Connecticut Attorney General Richard Blumenthal of the May theft of two company laptops containing personal information of 950 people. The earlier security breach exposed information on 17,000 people. In a letter to Pfizer employees, Lisa M. Goldman, out of Pfizer's privacy office, said two password−protected laptops owned by consulting firm Axia were stolen out of a car in Boston. The information contained employee names and Social Security numbers. Letters about the data breach were posted online by TheDay.com.
Letter to Connecticut Attorney General Richard Blumenthal:
http://media.theday.com/gbl/media/dynamic/pdfnews/pfizersblu menthal.pdf
Source: http://www.informationweek.com/management/showArticle.jhtml;jsessionid=ZGVEFEQKQYWI4QSNDLPSKH0CJUNN2JVN?articleID=201800113&articleID=201800113

7. *August 13, VNUNet* — **Poor company policy aids identity theft.** Many businesses are still in the dark ages when it comes to making sure customers are who they say they are, reveals a new report by risk management experts Experian. The report shows that 70 percent of financial services companies still rely on fraud−friendly paper documents to authenticate a person's identity, and 36 percent of retailers and 40 percent of telecommunications companies are still doing it. According to the survey too many industries are left hamstrung by their reliance on the use of passports, utility bills and driving licenses for authentication, despite the fact that

electronic systems are generally considered to be safer and faster for all concerned. "It's staggering to think that today's businesses are still using paper documents to confirm a person's identity," said Anne Green, fraud consultant at Experian. "Take passports for example. They actually date back to the 15th century and were intended for travel, not verifying a person who wants to open a bank account. Companies need to break the paper chain and move with the times. It is the 21st century after all."
Source: http://www.vnunet.com/vnunet/news/2196527/poor−company−policy−aids−identity−theft

8. *August 13, Federal Computer Week* — **DHS IG: Weak internal controls put financial data at risk.** The integrity of the Department of Homeland Security's (DHS) financial data is at increased risk because of weak information technology internal controls related to financial management systems, the DHS Office of Inspector General (IG) has said in a report. The report covers the IT management controls that support the department's financial statement for fiscal 2006. Internal controls reduce the risk of error or fraud in financial reporting.
IG Report: http://www.dhs.gov/xoig/assets/mgmtrpts/OIGr_07−53_Aug07.pdf
Source: http://www.fcw.com/article103492−08−13−07−Web

9. *July 13, Government Accountability Office* — **GAO−07−1014: Tax Gap: A Strategy for Reducing the Gap Should Include Options for Addressing Sole Proprietor Noncompliance (Report).** The Internal Revenue Service (IRS) estimates that $68 billion of the annual $345 billion gross tax gap for 2001 was due to sole proprietors, who own unincorporated businesses by themselves, underreporting their net income by 57 percent. A key reason for this underreporting is well known. Unlike wage and some investment income, sole proprietors' income is not subject to withholding and only a portion is subject to information reporting to IRS by third parties. The Government Accountability Office (GAO) was asked to (1) describe the nature and extent of sole proprietor noncompliance, (2) how IRS's enforcement programs address it, and (3) options for reducing it. GAO analyzed IRS's recent random sample study of reporting compliance by individual taxpayers, including sole proprietors. GAO recommends that the Secretary of the Treasury ensure that the tax gap strategy (1) covers sole proprietor compliance and is coordinated with broader tax gap reduction efforts and (2) includes specific proposals, such as the options in this report. GAO is not making recommendations regarding specific options. IRS and the Department of the Treasury provided technical comments on a draft of this report, which GAO incorporated as appropriate.
Highlights: http://www.gao.gov/highlights/d071014high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−1014

[Return to top]

Transportation and Border Security Sector

10. *August 15, Government Accountability Office* — **GAO−07−291R: Freight Railroads: Updated Information on Rates and Other Industry Trends (Correspondence).** The Government Accountability Office (GAO) was asked to update its October report using 2005 data, which became available after GAO issued the report. This report provides that update, including changes in industry and commodity rates, other costs to shippers (such as railcar ownership and miscellaneous revenue), and data on traffic traveling at rates equal to or greater

than 180 percent R/VC. Also, GAO is providing additional information and analysis of these data −− including rates, tonnage, and revenue from 1985 through 2005 −− in the form of an e−supplement, which can be viewed at GAO−07−292SP. In 2005, industry rail rates increased seven percent over their 2004 levels, the largest annual increase over the past 20 years, outpacing the rate of inflation for only the second time in 20 years. Rates also increased for the commodities GAO reviewed −− including such commodities as coal and grain. Freight railroad companies continued a 20−year trend of shifting other costs to shippers, including railcar ownership. While it remains difficult to precisely determine how many shippers are captive to a single Class I railroad because available proxy measures can overstate or understate captivity, 2005 data indicate that potentially captive traffic continued to drop.
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−291R

11. *August 15, Government Accountability Office* — **GAO−07−292SP: Freight Railroads: Electronic Supplement on Rates and Other Industry Trends, 1985−2005., (Special Report). [Internet only].** This e−publication supplements the Government Accountability Office (GAO) report "Freight Railroads: Updated Information on Rates and Other Industry Trends" by presenting an analysis of the Surface Transportation Board's (STB) Carload Waybill Sample. GAO analyzed the data in this database and present trends across the industry, for certain commodities, and by state. It is important to note that while this e−supplement provides useful information on the freight railroad industry, limitations exist, and therefore the data must be interpreted with caution. For example, it is possible for the data to show the R/VC ratio increasing, potentially indicating a lack of competitive alternatives for a shipper −− when the rate paid by the shipper is in fact declining. For a more detailed discussion of scope and methodology, including limitations of the data, please visit GAO's scope and methodology page. GAO performed this work from October 2006 through June 2007 in accordance with generally accepted government auditing standards.
Scope and methodology page: http://www.gao.gov/special.pubs/gao−07−292sp/osm.html
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−292SP

12. *August 15, Los Angeles Times* — **LAX outage is blamed on a single computer.** U.S. Customs officials said Tuesday, August 14, that they had traced the source of last weekend's system outage that left 17,000 international passengers stranded in airplanes to a malfunctioning network interface card on a single desktop computer in the Tom Bradley International Terminal at Los Angeles International Airport (LAX). The card, which allows computers to connect to a local area network, experienced a partial failure that started about 12:50 p.m. PDT Saturday, August 11, slowing down the system, said Jennifer Connors, a chief in the office of field operations for the Customs and Border Protection agency. As data overloaded the system, a domino effect occurred with other computer network cards, eventually causing a total system failure a little after 2 p.m., Connors said. "All indications are there was no hacking, no tampering, no terrorist link, nothing like that," she said. "It was an internal problem" contained to the Los Angeles International Airport system. The system was restored about nine hours later, only to give out again late Sunday for about 80 minutes. The second outage was caused by a power supply failure, Connors said.
Source: http://www.latimes.com/news/nationworld/nation/la−me−lax15aug15,1,6802259.story?coll=la−headlines−nation

13.

August 14, Department of Transportation — **Secretary of Transportation names five communities to receive funding to help fight traffic congestion.** Department of Transportation Secretary Mary E. Peters on Tuesday, August 14, announced she has selected five metropolitan areas across the country as the first communities to participate in a new federal initiative to fight traffic gridlock. This announcement follows an eight−month nationwide competition to select a handful of communities from among the 26 who applied to join the Department's Urban Partnership program, aimed to reduce traffic congestion using approaches like congestion pricing, transit, tolling, and teleworking. The Secretary said the communities, as winners of the competition, will receive the following funding amounts to implement their traffic fighting plans: Miami, $62.9 million; the Minneapolis area, $133.3 million; New York City, $354.5 million; San Francisco, $158.7 million; and the Seattle area (King County), $138.7 million. Secretary Peters said every Urban Partner proposed some form of congestion pricing. The Urban Partnership Program is part of the Bush Administration's comprehensive initiative launched in May 2006 to confront and address congestion throughout the nation's transportation system.
Source: http://www.dot.gov/affairs/dot8507.htm

14. *August 14, Associated Press* — **Unruly passenger on Las Vegas−bound flight faces federal charges.** An airline passenger accused of yelling profanities, making crude comments, and pushing a flight attendant on a Chicago−Las Vegas flight has been charged in federal court with interfering with flight attendants. Andy Lee Osuna, 29, was arrested Friday, August 10, after Southwest Airlines Flight 2275 was diverted to Denver. The flight crew had restrained him with flex cuffs. An arrest warrant affidavit released Tuesday, August 14, said Osuna denied yelling profanities and making crude comments and said he did not remember being handcuffed. The affidavit said Osuna told investigators he drank two malt liquors before the flight and had five cocktails on board. Osuna was being held without bond pending a detention hearing Friday.
Source: http://www.usatoday.com/travel/flights/2007−08−14−unruly−passenger−charged_N.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

15. *August 15, Associated Press* — **Colorado bull tested for tuberculosis.** A Colorado rodeo bull that has been in at least a dozen states is being tested for bovine tuberculosis. Colorado Agriculture Department spokesperson Christi Lightcap said the bull was tested because it came in contact with another bull that had the disease.
Source: http://www.coloradoan.com/apps/pbcs.dll/article?AID=/20070815/UPDATES01/70815007

16.

August 14, Horse.com — **Eastern equine encephalitis hitting Louisiana horses.** Eastern equine encephalitis (EEE) has caused the deaths of eight horses in Lafourche Parish, LA. Veterinarians also suspect the virus in two additional cases of equine illness. The progression of EEE is swift and ugly. Affected horses will struggle with muscle tremors, weakness, and staggering gaits, and they might circle aimlessly or tilt their heads at odd angles. Eastern equine encephalitis is of special interest to veterinarians and human health authorities, as the virus can also infect humans. The virus cannot pass directly from horses to humans.
Source: http://www.thehorse.com/ViewArticle.aspx?ID=10183

17. *August 14, Delta Democrat Times* — **Soybean rust discovered in Mississippi.** Agriculture researchers have been hoping there wouldn't be any Asian rust disease on Mississippi soybeans this year, but after months of keeping a close watch on crops throughout the state, they have now found it in their own front yard. Gabe Sciumbato, a plant pathologist, said the rust was discovered Sunday, August 12, on a sentinel plot at Mississippi State University's Delta Research and Extension Center in Stoneville. Last month some farmers in Louisiana, Texas and Arkansas found rust in their fields. It had not been found in Mississippi this year, but it was found in kudzu last month.
Source: http://www.ddtonline.com/articles/2007/08/14/news/news1.txt

[Return to top]

Food Sector

18. *August 14, U.S. Food and Drug Administration* — **Federal court issues permanent injunction against Puerto Rico dairies.** The U.S. District Court for the District of Puerto Rico issued an Order of Permanent Injunction against J.M. Dairy Inc. and Las Martas Inc., and Juan Manuel Barreto Ginorio, the owner of the dairies, after illegal drug residues were found in cows. The U.S. Food and Drug Administration (FDA) is concerned about the sale of animals for human food that may contain illegal levels of animal drugs because of the potential for adverse effects on human health. The order also prohibits the sale of milk until compliance is met. The court order follows a civil complaint filed against the defendants on September 19, 2006, based upon FDA's investigations into the dairies and their practices. The dairies produce milk for human consumption and sell dairy cows for slaughter for human consumption. The injunction is based, in part, on five illegal residues in the edible tissue of three dairy cows sampled by the U.S. Department of Agriculture's Food Safety Inspection Service (FSIS). The drug residues found by FSIS included antibiotics such as sulfamethazine, sulfathiazole, sulfadimethoxine, and penicillin at levels not permitted by FDA. More recent FDA inspections confirmed that the dairies continued to use animal drugs in a manner contrary to the label directions.
Source: http://www.fda.gov/bbs/topics/NEWS/2007/NEW01682.html

19. *August 13, Associated Press* — **Fish recalled.** Krasniy Oktyabr Inc. of Brooklyn, NY, is recalling packages of Herring of the Special Ambassador 7 Uzlov because the fish might be contaminated with Clostridium botulinum, which causes botulism, a potentially fatal form of food poisoning. No illnesses have been reported to date. The herring was distributed to retail stores in New York City.
Source: http://www.star−telegram.com/461/story/200654.html

[Return to top]

Water Sector

20. *August 14, Associated Press* — **Water utilities say most Australian cities must find new water supplies.** Nearly every Australian city will have to find new water supplies over the next decade, according to a study released Tuesday, August 14. The annual report by the Water Services Association of Australia found that after a decade of punishing drought, authorities in all of Australia's mainland capital cities will need to find new ways to provide water for residents, such as desalination and recycling, in the next five to 10 years. Hobart, the capital of the island state of Tasmania, is the exception and is expected to have sufficient water. In its report to urban water utilities, the association said water prices will rise steadily in cities to pay for new infrastructure in the driest continent in the world after Antarctica. The report found that in the fiscal year ending June 2007, rainfall in catchments serving towns and cities fell by as much as 80 percent below average.
Source: http://www.iht.com/articles/ap/2007/08/14/asia/AS−GEN−Australia−Water−Shortage.php

21. *August 14, New York Times* — **Water levels in three Great Lakes dip far below normal.** Water levels in the three upper Great Lakes are wavering far below normal, and experts expect Lake Superior, the northernmost lake, to reach a record low in the next two months, according to data from the international bodies that monitor the Great Lakes, the world's largest freshwater reservoir. Although the cause of the falling levels is in dispute, the effects in Lakes Michigan and Huron are visible everywhere. Ship channels are overdue for dredging. Wetlands in some areas like Georgian Bay, east of Lake Huron in Ontario, have dried up. Beaches around Saginaw Bay in Michigan have reverted to marshes as shorefront reverts to wetlands. One−third of the Michigan boat ramps are unusable. Evidence is growing that people caused some losses in Lakes Huron and Michigan. Gravel mining early in the 20th century by private companies and dredging by the Army Corps of Engineers, particularly in the mid−1960s, may have widened and deepened the St. Clair River, through which those two lakes drain into Lake Erie. The flow may be eroding the riverbed. The erosion may in turn result in increased outflow, more than can be replenished by rain or snowmelt, according to a study by Canadian coastal engineers.
Source: http://www.nytimes.com/2007/08/14/us/14lakes.html?em&ex=1187236800&en=ba25236bdc2b5500&ei=5087%0A

[Return to top]

Public Health Sector

22. *August 14, Voice of America* — **France reports bird flu.** French authorities say four ducks have tested positive for the H5N1 strain of bird flu in northeastern France. The ducks were found dead in an area known as Diane Capelle in the Moselle region. Two dead swans had already been discovered with bird flu at the end of July in the same area. That outbreak was the first in France in more than a year.

Source: http://www.voanews.com/english/2007−08−14−voa63.cfm

23. *August 14, Reuters* — **Size of blood donor pool has been overestimated.** The number of people in the U.S. who are available to donate blood is considerably overestimated. The current method of estimating the pool of eligible blood donors uses age as the only criterion for excluding people from donating blood. In reality, a number of other factors can lead to ineligibility. Researchers at the University of Minnesota created a model to help estimate the number of people in the U.S. who are not eligible for blood donation. Researchers note that in 2003, the U.S. population was approximately 294 million. Conventional methods would suggest that there would be 178 million eligible donors. Based on their model, however, researchers calculated that only 111 million persons were eligible.
Source: http://www.reuters.com/article/healthNews/idUSSCH47911320070 814

24. *August 13, Xinhua (China)* — **European Union develops new intelligence system to identify public health threats.** A medical intelligence system has been developed to help health authorities identify disease outbreaks or industrial accidents as early as possible and react promptly, the European Union's executive arm said Monday, August 13. The new system, called MediSys, can also provide invaluable information on how to tackle a major incident such as a bioterrorist attack, said the European Commission (EC). It said that the system can constantly collect and sort information from over 1,000 news and 120 public health Websites in 32 languages.
Source: http://mathaba.net/news/?x=560746

[Return to top]

Government Sector

25. *August 15, Department of Homeland Security* — **DHS Fact Sheet: National Applications Office.** The Department of Homeland Security's (DHS) National Applications Office is the executive agent to facilitate the use of intelligence community technological assets for civil, homeland security and law enforcement purposes within the United States. The office will begin initial operation by fall 2007 and will build on the long−standing work of the Civil Applications Committee, which was created in 1974 to facilitate the use of the capabilities of the intelligence community for civil, non−defense uses in the United States. While civil users are well supported for purposes such as monitoring volcanic activity, environmental and geological changes, hurricanes, and floods through the current Civil Applications Committee, homeland security and law enforcement will also benefit from access to Intelligence Community capabilities. As a principal interface between the Intelligence Community and the Civil Applications, Homeland Security and Law Enforcement Domains, the National Applications Office will provide more robust access to needed remote sensing information to appropriate customers.
Source: http://www.dhs.gov/xnews/releases/pr_1187188414685.shtm

26. *August 14, Federal Emergency Management Agency* — **Harvard University earns Stormready® distinction.** Harvard University was recently recognized as a StormReady® community −− the fifth in Massachusetts to do so. It is the first university in New England and

first of the Ivy League schools to attain this certification. This designation indicates that Harvard has fulfilled its emergency communications capabilities and preparedness responsibilities in the event of a natural disaster. The nationwide community preparedness program uses a grassroots approach to help communities develop plans to handle local severe weather and flooding threats. A StormReady® designation will be in effect for three years, after which time the university will go through a renewal process. The program is voluntary and provides communities with clear−cut advice from a partnership between local National Weather Service forecast offices and state and local emergency managers. StormReady® started in 1999 with seven communities in the Tulsa, OK, area. There are currently 1,208 StormReady® sites across the country, including 18 universities.
Source: http://www.fema.gov/news/newsrelease.fema?id=38630

[Return to top]

Emergency Services Sector

27. *August 15, Times Herald (MI)* — **Firefighters train with rail car.** Firefighters in Port Huron, MI, seized a rare opportunity Tuesday, August 14, to learn more about the hundreds of rail cars carrying freight that enter the city each day. CN Railway brought a specially−outfitted training car to the 16th Street Amtrak station, where firefighters participated in hands−on exercises. Port Huron fire Captain Mark White said the training allows firefighters to learn more about the systems, valves, and components of rail cars. Firefighters from all shifts will have a chance to attend the training during the next three days. Knowledge of rail−car systems is important to Port Huron's first responders. Local police and firefighters are charged with responding to incidents at the rail tunnel connecting Sarnia to Port Huron. The tunnel is one of the busiest international freight crossings in the United States, according to the United States Bureau of Transportation Statistics. The training car, called CN 911, is used for trainings across the United States and Canada. Palmer said it is in high demand and is booked for the next two years. It is scheduled to move on to Pontiac, MI, after the Port Huron training is finished.
Source: http://www.thetimesherald.com/apps/pbcs.dll/article?AID=/20070815/NEWS01/708150307/1002

[Return to top]

Information Technology and Telecommunications Sector

28. *August 15, IDG News Service* — **Citrix to acquire virtualization vendor XenSource for $500M.** Citrix Systems plans to acquire virtualization vendor XenSource for approximately $500 million to enable the application delivery software vendor to enter both the server and desktop virtualization markets. Citrix made the announcement on Wednesday, August 15, the day after XenSource's rival VMware launched an initial public offering.
Source: http://www.infoworld.com/article/07/08/15/Citrix−to−acquire− XenSource_1.html

29. *August 15, IDG News Service* — **Vulnerability uncovered within Yahoo Messenger.** A new vulnerability in Yahoo's instant messenger program can potentially cause unwanted code to run on a PC, according to security researchers. Details of the vulnerability were first posted on a

Chinese−language security forum and was later confirmed with Yahoo security officials, wrote Wei Wang, a researcher with McAfee's Avert lab in Beijing, on a company blog. So far, no exploit code has been published, wrote Karthik Raman, also of McAfee. The vulnerability affects Yahoo Messenger version 8.1.0.413. It is triggered when a user accepts an invitation to use their Web camera. The type of vulnerability is called a heap overflow, where a piece of code can be executed with improper permissions, which can allow for further malicious behavior such as downloading other code, said Greg Day, a security analyst for McAfee in the UK.
Source: http://www.infoworld.com/article/07/08/15/Vulnerability−in−Yahoo−Messenger_1.html

30. *August 15, Register (UK)* — **Webmail−creating Trojan targets Gmail.** A strain of malware capable of setting up bogus Hotmail and Yahoo! accounts in order to send spam has been adapted to also target Gmail accounts. The HotLan Trojan creates automatically−generated Webmail accounts, implying that spammers have discovered a means to defeat Captcha challenge−response systems. Captcha systems, which typically prevent accounts being created until a user correctly identifies letters depicted in an image, are designed to ensure requests are made by a human rather than an automated program. Since the arrival of the first variant of the Trojan last month, more than 500,000 spam e−mail accounts have been created, according to Romanian anti−virus firm BitDefender. A joint effort between the security teams of BitDefender and Yahoo! appears to have stymied attempts to generate and use Yahoo! accounts to send spam. However, this has pushed the problem onto Hotmail and Gmail (a new target of a latter variant of the Trojan) rather than having the desired effect of bringing the creation of bogus accounts under control.
Source: http://www.theregister.co.uk/2007/08/15/webmail_trojan_updat e/

31. *August 14, U.S. Computer Emergency Readiness Team* — **US−CERT Technical Cyber Security Alert TA07−226A: Microsoft Updates for Multiple Vulnerabilities.** Microsoft has released updates to address vulnerabilities that affect Microsoft Windows, Internet Explorer, Windows Media Player, Office, Office for Mac, XML Core Services, Visual Basic, Virtual PC, and Virtual Server as part of the Microsoft Security Bulletin Summary for August 2007. The most severe vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial−of−service on a vulnerable system. Solution: Microsoft has provided updates for these vulnerabilities in the August 2007 Security Bulletins. The Security Bulletins describe any known issues related to the updates. Administrators are encouraged to note any known issues that are described in the Bulletins and test for any potentially adverse effects.
Microsoft Security Bulletin: http://www.microsoft.com/technet/security/bulletin/ms07−aug.mspx
Updates for Microsoft Windows and Microsoft Office XP and later are available on the Microsoft Update site: https://www.update.microsoft.com/microsoftupdate/v6/muoptdefault.aspx?returnurl=https://www.update.microsoft.com/microso ftupdate&ln=en−us
Microsoft Office 2000 updates are available on the Microsoft Office Update site: http://office.microsoft.com/en−us/default.aspx
Apple Mac OS X users should obtain updates from the Mactopia Website: http://www.microsoft.com/mac/
System administrators may wish to consider using an automated patch distribution system such as Windows Server Update Services: http://technet.microsoft.com/en−us/wsus/default.aspx

Source: http://www.uscert.gov/cas/techalerts/TA07−226A.html

32. *August 14, eWeek* — **ATI driver bug leaves Vista open to attack.** Microsoft is working with AMD to fix a bug in an ATI driver that ships preinstalled on millions of laptops and which leaves the Vista kernel open to arbitrary memory writes by malicious driver authors. It's not just ATI −− virtualization security researcher Joanna Rutkowska said during her presentation at Black Hat earlier in August that ATI, which is owned by AMD, and Nvidia are just two examples of particularly badly written drivers, and that there could be tens of thousands of vulnerable drivers out there. The bug in the ATI driver is that it allows arbitrary memory writes. Malicious driver authors can use that flaw to load unsigned drivers via the standard loading mechanism.
Source: http://www.eweek.com/article2/0,1895,2170804,00.asp

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.

Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer